International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 3, Jun 2014, 139-148

TRANS STELLAR
• Journal Publications • Research Consultancy

COMPARATIVE STUDY OF COLLABORATIVE ATTACKS & SECURITY MECHANISMS IN MANET

AJAY DUREJA[1] & VANDNA DAHIYA[2]

[1]Assistant Professor, PDM College of Engineering for Women, Bahadurgarh, Haryana, India

[2]P.G Student, PDM College of Engineering for Women, Bahadurgarh, Haryana, India

ABSTRACT

Mobile Ad-hoc network is a infrastructure less network where communication takes place between collections of mobile hosts. There are several threats to ad-hoc network termed popularly as active and passive attacks. Collaborative attack is a new generation threat for ad-hoc networks. In collaboration attacks, multiple attackers synchronize their actions against some network to disturb the genuine communication. There are various vulnerabilities in the protocol suite due to which these attacks cause more danger to these networks. Unique characteristics of MANET topology such as open peer-to-peer architecture, dynamic network topology, shared wireless medium, mobility, self configuration and limited resources (battery, memory and computation power) pose a number of non-trivial challenges to security design. Security is a major concern for protected communication between mobile nodes in a hostile environment. Routing plays the key role in communication in these networks and thus also in the security of the network. In general, routing security in wireless MANETs appears to be a problem that is not trivial to solve. In this paper, we review some of the interactions among various Collaborative attacks like Blackhole attack, Sybil, Warmhole attack, DOM etc. We also study the work on securing the MANETs with different approaches like Cryptographic methods, Trust Based systems etc.

KEYWORDS: MANET, Collaborative Attack, Cryptography, Trust Based Systems, Hash Based Proof

INTRODUCTION

Mobile ad hoc network is an autonomous network where communication between various mobile nodes takes place over wireless link. Functioning in MANET depends on trust and cooperation among nodes as there is no central authorization for certificate of secure nodes. Various nodes help each other in managing the network and share the responsibility of conveying all this information to all other nodes across whole topology. Each mobile node acts as a host as well as a router and performs the functioning of routing and relaying the messages to the correct node in the network once a route is discovered. MANET is prone to larger security vulnerabilities and attacks because of certain features of MANET like-Mobility and self-configuring property which make it easy for intrusion, dynamic topology, no central authority, cooperation among nodes for relaying packets and assuming all nodes are secure, open-shared wireless network with no dedicated routers and switches. Low energy capacity is a well-known weakness explored by intruders. Routing protocols are focused on performance and do not have a complete formed Internet standard.

There are many other applications of MANET. For examples, MANET can be used to provide emergency services when the underlying infrastructure is damaged.[2] Various computer scientists have expected a world of omnipresent computing where, there would be computers all around us performing all the routine tasks to make our lives easier. These omnipresent computers connect in mobile ad hoc mode and change the environment or react to the change of

the environment where they are suited. MANET is also found useful during any environmental dangerous condition and acts as a sensor dust network where tiny sensor devices offer detailed information in such cases.

COLLABORATIVE ATTACKS

Due to the fact that MANET is a group of nodes that form a temporary network without centralized administration, the nodes have to communicate with each other based on unconditional trust. This characteristic leads to the consequence that MANET is susceptible to various attacks. The classification can be based on the behavior of the attack (Passive vs. Active), the source of the attacks (Internal vs. External), the processing capacity of the attackers (Wired vs. Mobile) and the number of the attackers (Single vs. Multiple). [3, 4, 5, 6] Other commonly observed misbehavior of nodes is packet dropping. In a practical MANET, most devices have very limited computing and battery power while packet forwarding consumes a lot of such resources. Thus some of the mobile devices would not like to forward the packets for the benefit of others and they drop packets not destined to them. These misbehaved nodes are very difficult to identify because we cannot tell that whether the packets are dropped intentionally by the misbehaved nodes or dropped due to the node having moved out of transmission range or other link error. Packet drop significantly decreases the network performance.

Collaborative attacks (CA) are new generation attack which can be defined as a homogeneous attack (i.e. blackhole or wormhole attack), involving two or more colluding nodes; classified as internal active attack that can be processed using wired or wireless link and triggered by single or multiple attackers. Each individual attacker may have specialized expertise. Multiple attacks occur when a system is disturbed by more than one attacker, but not necessarily in collaboration

There are various features of collaborative attack like attackers can launch sequential disruptions in short intervals so the target network is not able to respond in time, attackers can also concentrate on a group of nodes or spread to different groups of nodes just for confusing the detection/prevention system in place, attacks may be long-lived or short-lived ones, internal and external users can collaborate to launch attacks. For example- Black-hole attack where a node transmits a malicious broadcast informing that it has the shortest and most current path to the destination aiming to intercept messages. It can setup a route to some destination via itself and when the actual data packets get there they are simply dropped, forming a black hole where data enters but never leaves. [7,8]

Various attacks can be synchronized with one another to form a CA. Some of them are

Denial-of-Messages (Dom) Attacks: Harmful node prevents other honest destineds nodes to receive the data intended to receive by them.

Grey Hole: In this attack the enemy selectively drops some kinds of packets but not all. For example the attacker might drop data packets but forward control packets and routing packets. It can drop packets at some random time intervals only and not all the time.

Duplication Attacks: Adversaries can insert additional replicated hostile nodes into the network after obtaining some secret information from the captured nodes by receiving the data destined for original nodes.

Wormhole Attacks: An attacker records packets at one location in the network and tunnels them to another location. This kind of attack together with a partitioning attack can gain almost complete control over the network traffic.[9,10,11]

Sybil Attacks: A malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system. This way the malicious nodes can control the decisions of the system, especially if the decision process involves majority or any other type of collaboration [12].

Hastening Attacks: Using the fact that only the first message received by a node is used, preventing loops an attacker broadcast a malicious control messages fast enough to block genuine messages that arrive later.

Nasty Flooding: A bad node floods the network or a specific target node with data or control messages.

***Splitting of Network*:** Another kind of attack is for the attacker to create a network partition in which some nodes are split up to not being able to communicate with another set of nodes.

Resource Consumption: By injecting extra data packets or control packets into the Ad Hoc network limited resources such as bandwidth and maybe battery power are consumed for no reason.

Crashing Routing Traffic Attack: It is essential in the Ad Hoc network that all nodes participate in the routing process. However, a node may act selfishly and process only routing information that are related to itself in order to conserve energy. This type of attack can create instability in the network or even partition the network.

Position Disclosure: A location disclosure attack can reveal information related to the location of a node or the topology and structure of the network.

Example of Collaborative attack- *Joint black-hole and wormhole attack*

- Node A fools node S informing it has shortest path to D
- A forwards a packet to X
- X sets up a tunnel to Y
- Any further packet will now go through the tunnel
- In tunnel, packets can be selectively dropped or corrupted with.

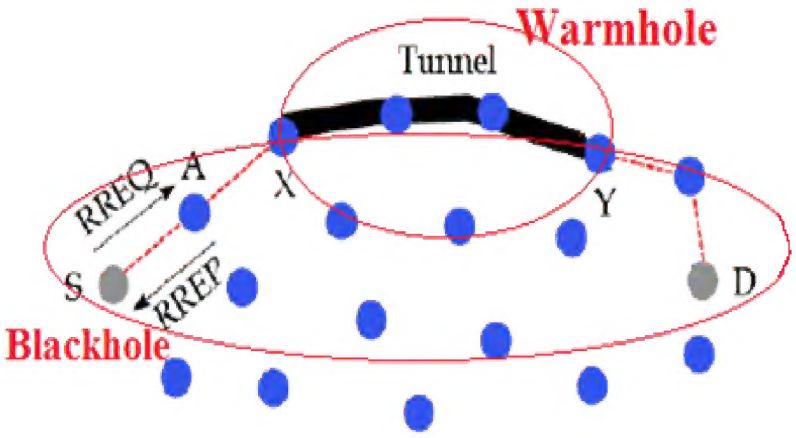

Figure 1

REVIEW OF VARIOUS SECURITY MECHANISMS

Various routing strategies have been proposed so far which might take security and QoS (Quality of Service) as the major concerns. Ensuring both of these parameters at the same time might be difficult. A very secure routing protocol surely incurs more overhead for routing, which might degrade the QoS level. So an optimal trade-off between these two parameters could be searched. A comparative study of various security mechanisms proposed so far incorporating in routing can be discussed [13,14,15,16].

Hash Based Node Behavioral Proofs

In the hash based proof, it was considered that all the intermediate nodes on a route to a specific destination D would be in memory of source S and with every intermediate node ni, S shares a unique symmetric key ki and a random number ri. Source and the intermediate nodes agree on h() which is a secure hash function and generated at each intermediate node according to this procedure-

Source node earlier decides the path and all the intermediate nodes and then source sends the sequence number of all the packets to first intermediate node ni. Along with this, a newly generated random number will be attached to the end of each packet. Now, the format of the sent packet is:

$S \rightarrow n1$: (S, D, data packet, random number $t0$) (1)

Node n1 now combine its random number r1 with the incoming packet and calculates t1 and is now ready to send this information to next intermediate node.

$t1 = h(S \| D \| \text{data packet} \| t0 \| r1)$ (2)

$n1 \rightarrow n2$: (S, D, data packet, $t1$) (3)

where "||" represents the concatenation operation. The procedure keeps going on all the intermediate nodes. Every node ni feed the received data packet and *ti* to the Bloom filter to update the node behavioral proof. The process remains continue until all packets sent by *S* have been received and the behavioral proof has been generated. Node ni will then encrypt the proof with the key *ki* and send it back to the source. Source S receives the data sent by intermediate nodes and verify the correctness of node behavioral proof. S can also reconstruct the assurances of the packets and generate its own copy of the Bloom filter. It will then compare this value to the received behavioral proof. If the difference of both the values is more than a specified value *S* will conclude that the disobedient node is in the segment from S to ni otherwise, the attacker is in the segment from *ni* to *D*. Both type of information is needed in this type of approach, intermediate nodes information and data packets.

DISCUSSIONS

Hash functions are difficult to calculate at every intermediate node and introduce severe overhead. Also it is not suitable for low bandwidth networks as intermediate node needs to send sixteen more bytes for every data packet. Also it is not suitable for low processing devices as hash function needs about 20 machine cycles to process one byte. Still, it was noticed that has function method can use to defend some of the collaborative attacks with the cost of extra communication.[17] But it can not defend against Denial of Service attack because malicious node can try to adjust their behavior according to hash based rules and can notify other attackers also.[18]

Reputation System and Trust Management Systems

These systems were discovered to resolve the problem of authorization of nodes. Stranger nodes are given the ratings of how trustworthy they are. They are different from normal MANET reputation systems where decentralization concept is used. Each node keeps rating of trust for other node based on the information supplied by other neighboring nodes or information supplied by trusted nodes. They also encourage untrustworthy node to behave trustfully.

Reputation systems rate how well a node behaves whereas trust rating shows how honest a node is While Reputation system is a global system and mobile nodes share their own familiarity of interaction with other nodes. The trust management system is a local reputation system where own observation of a node is used to rate the trust ability of other nodes in the network. It is also used to speed up the detection process as it is a local system to detect malicious nodes. Trust ratings are managed by trust managers in the network. These ratings give estimation of how trustworthy a node is. It is then used as an alternative approach to decide whether to accept the information from such nodes.

Example of Reputation System

CONFIDANT - CONFIDANT stands for Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Network. It is used in MANET with the aim of coping with malicious node. It is an example of reputation system. It is used in on demand routing protocols where the detected malicious nodes are not used for communication or packet forwarding.

CONFIDANT works to ease the mischief behavior of a node in following way- When a node sends a packet to its next hop which is then supposed to forward the packet, the node then notices whether the forwarding node forwards the packet by listening the packet in immoral way called as Passive Acknowledgement. If it is done so, the reputation rating about the hop node is increased and the first hand knowledge is then circulated about that node. If the packet is not listen by the hop node in certain period of time, the reputation rating of the hop node is decreased and the information is circulated that the node is misbehaving. A misbehaved threshold is defined which is used to compare the reputation rating about a node. If the node's behavior is below than this threshold value then the report is dent to Path Manager which then takes further actions. All the nodes circulate the information they have about their next hops or neighboring nodes. It is very important to know that with CONFIDANT a node only forwards or responds to nodes with good behavior. Therefore, this system isolates misbehaved node.

Example of Trust Management System

Trusted AODV

It is extension of AODV where opinion of a particular node is formed based on the opinions of all other nodes. All the operations performed by a node are observed and noted carefully. If the communication done by a node is well, its opinion is increased from other nodes' points of view otherwise if it does some malicious behavior, the opinion is formed with negative values and ultimately the node is denied by whole network. The opinions are updated frequently and are dynamic in nature. [19]

DISCUSSIONS

TAODV has to updates the opinions or generates certificate of correctness frequently which greatly increases the overhead of computation.

Cryptographic Methods

Several cryptography based routing protocols have been proposed based on the modification of existing ad hoc network routing protocols. Cryptographic methods have been employed in the existing protocols by extended them. Some of them can be described in brief as follows.[20,21,22]

Ariadne

Ariadne uses MACs and shared keys to authenticate a node in the network for communication among the nodes. It uses TESLA broadcast authentication protocol for authentication of routing messages. It is developed based on the DSR protocol and uses timestamps to prevent the looping of a paceket.

The drawback with this system is that it only takes care of route information like Denial of service attack but susceptible to Wormhole attacks as it does not detect whether the messages are received or dropped. It only checks whether the route information is compromised or not.

ARAN: Authenticated Routing for Ad hoc Network

It uses public key cryptography and a central certification authority server (third party) for node authentication and neighbor node authentication while discovering the routes. It is susceptible to Denial-of-service attack, Tunneling attack and Wormhole attack.

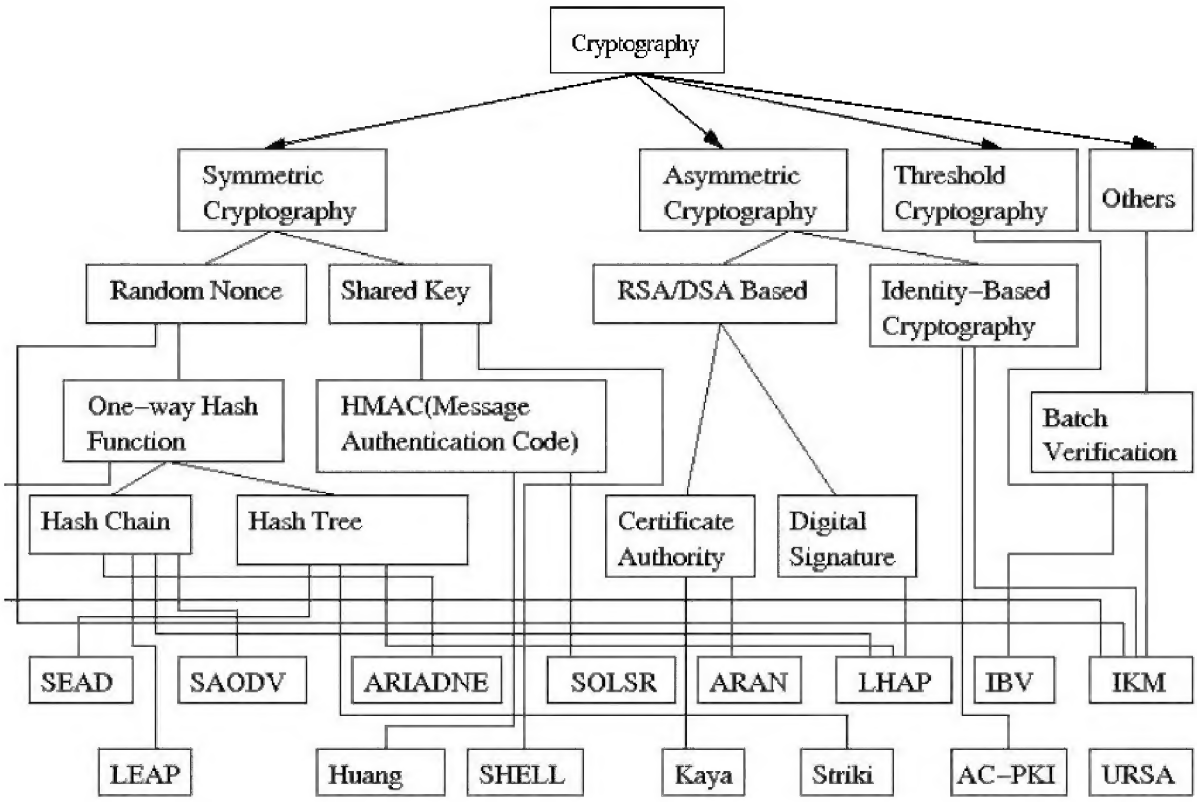

Figure 2: Cryptography Techniques Used in MANETs

Key Management System - Threshold Cryptography

A cryptographic scheme usually requires a key management service. Zhou et al proposes a key management system where keys are distributed using a public key infrastructure. Servers are destined to manage the distribution of these

keys with a scheme called as threshold cryptography scheme e.g. create a digital signature, so that any n+1 parties can perform this operation jointly but it is infeasible for at most n parties to do so, even by collusion. With threshold cryptography, each server has a public/private key pair. All nodes in the system know the public key of the service and rely on any certificates signed using corresponding private key. The scheme divides the private key k of the service into s shares, assigning one share to each server. Then with n + 1 correct partial signatures the combiner is able to compute the signature for the certificate. However compromised servers cannot generate correctly signed certificates because there are at most n of them. [23]

SAODV: Secure Ad hoc On-Demand Distance Vector Routing

It uses a central key management in its routing topology. 1024-bit RSA key pair is generated by the AODV and then securely bound global and local IPv6 addresses are generated using the public key of this pair. Digital signatures are used to authenticate at node level.[24]

There is much less per-packet overhead for TAODV compared to SAODV. SAODV is more expensive protocol and takes 2.35 times as long as AODV[25]; TAODV where takes only 1.11 times as long as AODV.

It shows that the trust-based calculations and additional information exchange can be used without incurring the overhead of SAODV.

DISCUSSIONS

Comparing to other security mechanisms, the cryptography systems have the advantage that they can cope well with DOS attack and all forms of the modification of messages. But they cannot cope well with packet drop attack as cryptography information in that case is also dropped. Presently there are two systems of cryptography, public key cryptography and identity-based (ID-based) cryptography both having their drawbacks that, in public key cryptography system, a certificate authority (CA) is required to issue certificates between users' public keys and private keys to ensure their authenticity, whereas in an ID-based cryptography system, users' private keys are generated by a key generation center (KGC), which means the KGC knows every users' keys (the key escrow problem).

Improved Route Discovery Schemes

Most existing routing protocols proposed for MANETs use flooding as a broadcast technique for the propagation of network control packets; a particular example of this is the broadcasting of route requests (RREQs), which facilitate route discovery.[26][27] The nodes which are out of transmission range in MANET can be accessed by routing through intermediate nodes. Often, hosts in a MANET operate with limited batteries and can roam freely towards any direction at any speed. The power exhaustion of some nodes and the mobility nature of nodes cause frequent topology changes. So the path between nodes or group of nodes may change periodically. The node which wants to transmit data packets first needs to discover the route to the destination using route discovery process of different routing protocols. So the route needs to be discovered with longer route lifetime with fewer changes.

As the route consists of number of wireless links, the route lifetime depends on the life time of nodes and individual links. The route discovery without considering the lifetime of the route leads to frequent failure. An improved scheme has been proposed to reduce the communication overhead incurred during the route discovery process and to impart only secure nodes for routing called as Fresh Algorithm.

Fresher Encounter Search (FRESH),[28] a simple algorithm for efficient route discovery in mobile ad hoc networks. Here nodes keep on discovering the route in iterations. Whenever a node wants to send data to some destination, it looks for an intermediate node which has already sent data to that destination. The intermediate node then looks for a node which sent data to destination more recently then this intermediate node. This process keeps on iterated until they get a path to the destination. FRESH replaces the single network-wide search of current proposals with a succession of smaller searches, resulting in a cheaper route discovery.

DISCUSSIONS

Routes obtained in this algorithm are loop-free. Another novel aspect of this algorithm compared to geographic algorithms, is that it does not assume any hardware add-ons such as GPS receivers.

CONCLUSIONS

Our objective of this paper is to provide a big picture of CAs'. Lots of techniques are reviewed with which some of the collaborative attacks can be defended with and easy detection is possible of most of the attacks. But all the previous approaches are vulnerable to complete set collaborative attacks. No protocol is fully secure from attacks being encountered. The study here establishes the foundation for future work towards designing more mechanism to identify the nodes and the links which are actively involved in the collaboration attacks. We can investigate other collaborative attacks and integrate various detection methods with secure routing protocols. We can incorporate more secure cryptographic techniques and ensure security by improving Route Discovery Schemes.

REFERENCES

1. Tamilselvan, L.; and Sankaranarayanan, V. (2007). Prevention of blackhole attack in MANET. The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications. Aus Wireless, 21-21
2. Manel Guerrero. Secure ad hoc on-demand distance vector (SAODV) routing, August 2001. INTERNETDRAFT draft-guerrero-manet-saodv-00.txt.
3. Yu, H., Gibbons, P. B., Kaminsky, M., and Xiao, F. SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks. In Proceedings of the 2008 IEEE Symposium on Security and Privacy (May 18 - 21, 2008). SP. IEEE Computer Society, Washington, DC, 3-17.
4. E. Hansson, J. Gronkvist, K. Persson and D. Norquist, "Specification-based Intrusion Detection Combined with Cryptography Methods for Mobile Ad hoc Networks", Technical Report. Available: http://www2.foi.se/rapp/foir1867.pdf. [Accessed May 15, 2009].
5. K. Hoffman, A. Ondi, R. Ford, M. Carvalho, D. Brown, W. H. Allen and G. A. Marin, "Danger theory and collaborative filtering in MANETs", Journal in Computer Virology, August 2008.
6. M. Workman, R. Ford and W. Allen, "A Structuration Agency Approach to Security Policy Enforcement in Mobile Ad Hoc Networks", Information Security Journal: A Global Perspective, Volume 17, Issue 5 & 6 2008, pages 267 – 277, January 2008.

7. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon and K. Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", Accessed May 2009 at

   http://cs.ndsu.edu/~nygard/research/BlackHoleMANET.pdf

8. S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour and Y. Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method",International Journal of network Security, Vol.5, No.3, PP.338–346, Nov. 2007.

9. M. A. Gorlatova, P. C. Mason, M. Wang, L. Lamont and R. Liscano, "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis", In Proceeding of Military Communications Conference, 2006. MILCOM 2006. IEEE, 23-25 Oct. 2006, Pages: 1-7, ISBN: 1-4244-0617-X

10. H. Vu, A. Kulkarni, K. Sarac, N. Mittal. "WORMEROS: A New Framework for Defending against Wormhole Attacks on Wireless Ad Hoc Networks". In Proceedings of International Conference on Wireless Algorithms Systems and Applications, LNCS 5258, pp. 491-502, 2008.

11. R. Maulik, N. Chaki. "A Comprehensive Review on Wormhole Attacks in MANET". In Proceedings of 9th International Conference on Computer Information Systems and Industrial Management Applications, pp. 233-238, 2010.

12. Yu, H., Gibbons, P. B., Kaminsky, M., and Xiao, F. SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks. In Proceedings of the 2008 IEEE Symposium on Security and Privacy (May 18 - 21, 2008). SP. IEEE Computer Society, Washington, DC, 3-17.

13. Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth Belding-Royer. A secure routing protocol for ad hoc networks. In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP 02), November 2002.

14. Manel Guerrero Zapata and N. Asokan. Securing ad hoc routing protocols. In Proceedings of the ACM Workshop on Wireless Security (WiSe 2002), September 2002.

15. Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Rushing attacks and defense in wireless adhoc network routing protocols. In Proceeding of the ACM workshop on WIreless SEcurity WISE 2003, San diego, CA, USA, september 2003.

16. Seung Yi, Prasad Naldurg, and Robin Kravets. Security-aware ad-hoc routing for wireless networks. In ACM Workshop on Mobile ad hoc networks, Mobihoc, 2001.

17. B. Preneel, et al, "Performance of optimized implementations of the nessie primitives," Deliverable 21 from the NESSIE IST FP5 project, 2003.

18. M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and efficient key management for access hierarchies," ACM Trans. Inf. Syst. Secur., 12(3):1–43, 2009.

19. K. Meka, M. Virendra, and S. Upadhyaya. Trust based routing decisions in mobile ad-hoc networks. In Proceedings of the Workshop on Secure Knowledge Management (SKM 2006), 2006.

20. Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth Belding-Royer. A secure routing protocol for ad hoc networks. In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP 02), November 2002.

21. S.S.Al-Riyami K.G.Paterson. Certificateless public key cryptography. page 452C473. C.S. Laih (ed.) Advances in Cryptology C Asiacrypt 2003, Lecture Notes in Computer Science, 2003.

22. Adi Shamir. Identity-based cryptosystems and signature schemes. Advances in Cryptology –Crypto '84, Lecture Notes in Computer Science 196, pages 47–53, 2005.

23. Y. Desmedt and Y. Frankel. Threshold cryptosystems. In CRYPTO, 1989.

24. M. G. Zapata and N. Asokan. Securing ad hoc routing protocols. In WiSE '02: Proceedings of the ACM workshop on Wireless security. ACM Press, 2002.

25. Charles E. Perkins and Elizabeth M. Royer. Ad hoc on-demand distance vector routing. In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999.

26. P. V. Jani, "Security within Ad-Hoc Networks," Position Paper, PAMPAS Workshop, Sept. 16/17 2002.

27. Minematsu, M., et al. HOWL: an efficient route discovery scheme using routing history in ad hoc networks. In 27th Annual IEEE International Conference on Local Computer Networks (LCN'02) 2002.

28. D. C. Y. Sasson and A. Schiper. Probabilistic broadcast for flooding in wireless mobile ad hoc networks. Technical Report IC/2002/54, EPFL, 2002.